UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,083	10/16/2000	Craig L. Ogg	40630/RRT/S850	2004

23363 7590 12/30/2009
CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
AUGUSTIN, EVENS J	
ART UNIT	PAPER NUMBER
3621	
MAIL DATE	DELIVERY MODE
12/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CRAIG L. OGG, and
WILLIAM W. CHOW

Appeal 2009-000120
Application 09/690,083
Technology Center 3600

Decided: December 30, 2009

Before, HUBERT C. LORIN, JOSEPH A. FISCHETTI, and BIBHU R. MOHANTY, *Administrative Patent Judges*.

FISCHETTI, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants seek our review under 35 U.S.C. § 134 (2002) of the Examiner's final rejection of claims 1-120. We have jurisdiction under 35 U.S.C. § 6(b)(2002).

SUMMARY OF DECISION

We AFFIRM IN PART.

THE INVENTION

Appellants claim a system and method for secure printing of value-bearing items (VBI) preferably, postage and to a cryptographic module for secure printing of VBIs. Specification 1:24-27.

Claim 1, reproduced below, is representative of the subject matter on appeal.

1. A cryptographic device for securing data on a computer network comprising:

- a processor programmed to authenticate a plurality of users on the computer network for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands;
- a memory for storing security device transaction data for ensuring authenticity of
    - a user,
        - wherein the security device transaction data is related to the one of the plurality of users;

- a cryptographic engine for cryptographically protecting data; and
- an interface for communicating with the computer network; wherein the cryptographic device is located remotely from the plurality of users; and
  - wherein once the user is authenticated,
  - the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user.

THE REJECTION

The Examiner relies upon the following as evidence of unpatentability:

Leon	US 6,424,954 B1	Jul. 23, 2002
Gravell	US 6,546,377 B1	Apr. 8, 2003

The following rejection is before us for review.

The Examiner rejected claims 1-120 under 35 U.S.C. 103(a) as being unpatentable over Leon in view of Gravell.

ISSUE

Have Appellants shown that the Examiner erred in rejecting claims 1-120 under 35 U.S.C. 103(a) as being unpatentable over Leon in view of Gravell on the grounds that a person with ordinary skill in the art would understand that a collection of servers working together in unison constitutes a processor; and whether a person with ordinary skill in the art would not think to combine the virtual system of Gravell with the physical meter system of Leon because Gravell teaches away from the use of a physical meter system?

PRINCIPLES OF LAW

Obviousness

> Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 550 U.S. at 407. ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.")

Novelty/Obviousness Nonfunctional Descriptive Material

When "non-functional descriptive material" is recorded or stored in a memory or other medium (*i.e.*, substrate) it is treated as analogous to printed matter cases where what is printed on a substrate bears no functional relationship to the substrate and is given no patentable weight. *See In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983).

Nonfunctional descriptive material cannot render nonobvious an invention that would have otherwise been obvious. *In re Ngai*, 367 F.3d 1336, 1339 (Fed. Cir. 2004). Patentable weight need not be given to descriptive material absent a new and unobvious functional relationship between the descriptive material and the substrate. *See In re Lowry*, 32 F.3d 1579, 1582-83 (Fed. Cir. 1994).

FINDINGS OF FACT

We find the following facts by a preponderance of the evidence:

1. Appellants' Specification does not specifically define the term "processor", nor does it utilize the term contrary to its customary meaning.

2. An ordinary and customary definition of the term "processor" as defined by Merriam Webster's Collegiate Dictionary Tenth Edition is: "COMPUTER".

3. The Examiner found:

> Leon fails to teach a system programmed to authenticate a plurality of user for secure processing if a value bearing item and memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a the cryptographic module is remotely located from the user wherein once the user is authenticated. However, Gravell et al teaches a system programmed to authenticate a plurality of user for secure processing if (sic of) a value bearing item and memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users and a the cryptographic module is remotely located from the user wherein once the user is authenticated (*see* abstract, fig 1, column 6 line 20-7 line 54).

Answer 4

4. The Examiner therefore concluded that:

> Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Gravell et al's a system programmed to authenticate a plurality of user for secure processing if a value bearing item and memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of

> users and a the cryptographic module is remotely located from the user wherein once the user is authenticated because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system thereby eliminated stolen and relocated meter problems and simplifies meter management in general.

Answer 4

5. Gravell discloses a data center which collectively processes transactions from a plurality of users and has a cryptographic engine for cryptographically protecting data in that:

> … the mailer initiates a postage evidencing transaction by running client software in PC 20, which contacts Data Center 30. At Data Center 30, a Communication Server 32 supports connectivity from various communication technologies and protocols. The Communication Server merges all incoming traffic and routes it to a Function Server 34, which supports mailer sign-on, postage dispensing and postal reporting. All mailer information, including use of public or private keys, is accessed from a Database Server 36 where the mailer information is securely stored using secure cryptographic processes and protocols. (It will be understood that, for security purposes, some information may be stored in a secure device or location, such as the Key Management System 38.) All sensitive cryptographic processes occur in the Key Management System 38, which includes a secure, tamper-evident and tamper-responding enclosed area. (col.7, ll. 20-36)

6. The Examiner found that Leon discloses a "…,system wherein a processor include a state machine for determine a state corresponding to availability of one or more commands, the cryptographic device enters an operational state in which it

continues to authenticate the user with respect to one or more transactions requested by the user (*see* Abstract, figs 5a -7, column 9 line 35-6)." Answer 24.

7. Leon discloses a state machine for determining a state corresponding to availability of one or more commands in that:

> (35) In a specific embodiment, the SMD includes two types of operating state: persistent states and intermediate states. A persistent state is one in which the SMD may remain for an indefinite period of time, even if power is removed and reapplied. An intermediate state is one that the SMD occupies for a short period of time, and is not occupied by the SMD upon power-up. Intermediate states are reached during transactions that include the transmission of more than one request/response message pair. In an embodiment, if the SMD is in an intermediate state and an unexpected event occurs (*e.g.*, power is removed or an unexpected message is received), the SMD reverts, when operation resumes, back to the previous persistent state it occupied prior to the beginning of the transaction.

Col.9, ll. 45-58.

8. The Specification describes a Postal Server as comprised of many servers such that

> …all of the business logic is processed in the servers and not in the database. By locating the transaction processing in the servers, increases in the number of transactions can be easily handled by adding additional Servers. Also, since each transaction is stateless (the application does not remember the specific hardware device the last transaction utilized), multiple machines can be added to each subsystem in order to handle increased loads. In one embodiment, load balancing hardware and software techniques are used to distribute traffic among the multiple servers. Specification 22: 24-34.

9. The Specification describes "a system which utilizes a plurality of cryptographic modules that need to work in concert. This entails creating a shared secret for all the modules." Specification 40:3-5

10. Leon discloses operational state commands including session management commands which allow processing between a host PC and the SMD in that:

> … messages are structured into groups called transactions. A transaction is a series of one or more request/response message pairs comprising the performance of a particular service. A request message is a message sent from the host PC to the SMD. A response message is a message sent from the SMD to the host PC following the SMD's processing of the request message. (col. 11, ll. 44-50)

11. The Examiner found with respect to claims 12, 13 17, 18 that Leon discloses the features of these claims (Answer 5-7) in that Leon discloses:

> The SMD does not accept a request to perform any transaction other than an Initialization transaction if it is in the Uninitialized state. After a successful Initialization transaction, the SMD transitions to the Initialized state. The SMD tests for the presence of the FIT flag when a request is received to perform any transaction that alters the SRDIs. If the FIT flag is present and the requested transaction is not the Initialization transaction, the SMD enters the Faulted state.
>
> In summary, the following operations are performed by the Initialization transaction:
>
> Load the DSA parameters p, q, and g into the SMD. Load the Provider X.509 certificate that includes the provider's public key into the SMD. Instruct the SMD to generate a public/private key pair. Instruct the SMD to export the public key.

> Place the SMD the Initialized operating state.
>
> Registration transaction: A Registration transaction prepares the SMD for operation at a user site and notifies the system server to activate the user's account. In an embodiment, registration of the SMD is performed before the SMD is allowed to process other transactions. The Registration transaction is achieved between the host PC, SMD, and system server via the SMD's main port. The following is a specific implementation of the Registration transaction, and other implementations are available.
>
> FIGS. 5C and 5C-2 show a flow diagram of an embodiment of the Registration transaction. At a step 550, the user requests, via the host PC, registration of the SMD. The user typically initiates an online registration when the user first installs the application software on the host PC. In response, the host PC sends the SMD a registration request message that includes the SMD X.509 certificate, at a step 552. This request message is signed using the provider's private key. The SMD receives and validates the request message, at a step 554.
>
> (Leon, col. 13, l. 63- col.14, l.31)

ANALYSIS

We affirm the rejection of claims 1-33, 35-120, and reverse as to claim 34.

The Appellants assert error with respect to claim 1 arguing that the Examiner has contradicted himself in the record as to what Leon does and does not teach. Appeal Br. 5-6.

We disagree with Appellants. While some findings regarding Leon appear inconsistent in the pre-Answer record, we do not find that such inconsistencies rise to the level of error because the Examiner's Answer is without contradiction on

this point. Specifically, in the Answer, the Examiner sets forth findings which distinctly delineate what Leon does and does not teach. FF 3. The Examiner in turn relies on Gravell to teach a system programmed to authenticate a plurality of users for secure processing of a value bearing item and a memory for storing security device transaction data for ensuring authenticity of a user. FF 4. From this standpoint, the Examiner's Answer clearly sets forth what each reference does and does not teach, and thus we do not find error with the rejection.

With that said, Appellants further argue that Leon fails to disclose "that the SMD of Leon includes a processor that supports a state machine, as recited in claim 1." Appeal Br. 5. We disagree with Appellants because the Examiner found that Leon discloses a "…system wherein a processor include[s] a state machine for determine[ing] a state corresponding to availability of one or more commands, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user." FF 6. A review of Leon shows the Examiner's finding to be correct because Leon discloses a state machine for determining a state corresponding to availability of one or more commands, namely, the operating state commands for a persistent state and an intermediate state. FF 7.

Appellants next argue that

> ...Gravell does not teach a system with a cryptographic device having a processor 'to authenticate a plurality of users ... for secure processing of a value bearing item' and having a 'cryptographic engine for cryptographically protecting data.' Rather, Gravell discloses a system where these functions are performed by separate servers, a function server and a key management server.

Appeal Br. 6. We disagree with Appellants because Appellants seek a definition of

the term "processor" to mean a single device located at a single server. However, we find that Appellants' Specification does not specifically define the term "processor", nor does it utilize the term contrary to its customary meaning. FF 1. An ordinary and customary definition of the term "processor" as defined by Merriam Webster's Collegiate Dictionary is generally stated as a "COMPUTER". FF 2. Gravell discloses a data center which collectively processes traffic from a plurality of users and has a cryptographic engine for cryptographically protecting data. FF 8-9. Appellants' own Specification suggests that Appellants' system similarly works within a system of servers with shared processing responsibilities. FF 5 which would suggest that the claimed "processor" is more of a collective processing, than the device specific type argued by Appellants.

Appellants next argue that "…one of ordinary skill in the art would not think to combine the virtual system of Gravell with the physical meter system of Leon because Gravell teaches away from the use of a physical meter system." Appeal Br. 7. We disagree with Appellants because Gravell does not actually teach away from *every aspect* of *all* SMD processing aspects. *See In re Gurley*, 27 F.3d at 553. For example, the Examiner found that both Gravell and Leon are directed to using computers having user authentication features to process value bearing items, e.g., postage meter printing. FF 3. Thus, as long as the combination is not directed to the discouraged aspects of the particular postage printing metering process, there is no teaching away.

Appellants also argue that:

> [B]y making the postage metering system of Leon remote from the user, the user is not able to locally access or use the physical meter of Leon in combination-with a scale plugged in to the physical meter or in combination with a printer that is part of the physical meter as

taught by Leon.
Appeal Br. 7. We disagree with Appellants because as modified, Leon would still provide the metering capabilities it possessed prior to modification. Appellants' argument effectively seeks an explanation of how the metering system would be bodily incorporated into the existing device which is not the test for obviousness. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

Claims 6 and 7

Claims 6 and 7 recite in pertinent part: wherein the state machine includes an exporting shares state; and an importing shares state. The Examiner found that Leon discloses this feature. Appellants argue that "[t]he sections of Leon relied upon by the Examiner do not mention such states or the use of shares." Appeal Br. 8. While there may not be an explicit disclosure of shares in Leon, we find that the combination of Leon and Gravell would have present some form of shared states being exported and imported given that a Communication Server 32 supports connectivity from various communication technologies and protocols and merges all incoming traffic and routes it to a Function Server 34. FF 11. Given the broad scope of these claims and the disclosed collective processing found in Gravell, we sustain the rejection of claims 6 and 7.

Claims 11, 12, 13 16, 17 and 18

The Examiner found with respect to claims 12, 13 17, 18 that Leon discloses at least one of the commands listed in these claims. FF 11. We find that claims 12, 16, 17, and 18 require at least a log on or log off command; claim 13 requires at least an open or close session command; and claim 11 requires at least an operational state command for session management. Appellants argue that "the cited sections of Leon relate to an Initialization transaction and Registration

transaction…", rather than the claimed commands. Appeal Br. 8-10. We disagree with Appellants.

With regard to those claims requiring at least a log on or log off command, we find that Initialization transactions would inherently need to include log on/off commands to signify the beginning and ending of the involved transaction such as where a Registration transaction prepares the SMD for operation at a user site and notifies the system server to activate the user's account. FF 11. "…Claim limitations not expressly found in [a]… reference are nonetheless inherent in it." *In re Cruciferous Sprout Litig.,* 301 F.3d 1343, 1349 (Fed. Cir. 2002) (citations and internal quotation marks omitted). "Under the principles of inherency, if a structure in the prior art necessarily functions in accordance with the limitations of a process or method claim of an application, the claim is anticipated.." quoting In re King, 801 F.2d 1324; (Fed. Cir. 1986).

Likewise, regarding the open/close session commands recited in claim 13, we find that such commands are also inherent to transactions in Leon, because transactions, such as Initialization and Registration, would require some signal or command given to the communicated with sever at the beginning and ending of the Initialization or Registration sessions. We have above addressed the issue of shares as recited in claims 6 and 7, and thus further find that Gravel would direct commands, such as log on and log off, in a shared manner as discussed above.

Regarding the requirement of claim 11 of operational state commands, we find that the process of effecting communication between the host PC and the SMD in Leon is an operation state, with the underlying transaction commands of each session or transaction controlling session management. FF 11. Thus, the requirements of claim 11 are met by Leon.

For the reasons set forth above, we likewise sustain the rejection of claims 57,84, 58,85, 61,88, 62,89 and 63,90 which contain corresponding limitations recited in claims 11, 12, 13 16, 17 and 18.

Claims 23 and 94

We find that the feature of a "computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user" would be a predictable way of processing transactions from multiple users in the combination of Leon and Gravell in order to keep track of each user's use separately. "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). Therefore we sustain the rejection of claims 23 and 94.

Claims 28 and 30-33, 69, 71, and 99

Appellants seek to distinguish these claims by the content which is contained in the value bearing item. We decline to accept this position because we find that items, such as a ticket or coupon, are only distinguishable by content, and thus such a distinction is based on non-functional descriptive material which cannot form a basis for patentability.

Claim 34

Claim 34 requires a security device transaction data having an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a

passphrase repetition list. The Examiner cites to column 42 of Leon to teach these features. Answer 9, items such as, the indicium key certificate serial number and passphrase repetition list are not disclosed and are not addressed by the Examiner. Therefore, we will not sustain the rejection of claim 34.

Claim 36

Claim 36 recites "wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices." We find this language to be functional. As functional language, we are required only to give the language weight to the extent that the prior art is or is not capable of meeting the limitation. *In re Schreiber*, 128 F.3d 1473, 1477-78 (Fed. Cir. 1997). Since we found that Gravell discloses a data center which collectively processes traffic from a plurality of users (FF 5), Gravell would thus also be capable of sharing a secret with a plurality of other cryptographic devices. Therefore we sustain the rejection of claim 36.

Claims 41 and 103

Representative claim 41 recites "at least one of the plurality of users is an enterprise account." Appellants' attempt to distinguish over the type of account in Leon is unpersuasive because it is a distinction based on content. We decline to accept this position because we find that items, such as account names, are only distinguishable by content, and thus such a distinction is based on non-functional descriptive material which cannot form a basis for patentability.

Claims 2-5, 8-10, 14, 15, 19-22, 29, 35, and 37-40

Appellants argue the patentability of these claims based on the arguments advanced for claim 1 which we found unpersuasive. For the same reasons, we will not sustain the rejection of these claims either.

Claims 42, 72 and 104

Representative claim 42 recites in pertinent part "authenticating the plurality of users for secure processing ... using one of a plurality of cryptographic devices." Appellants argue that neither "Leon or Gravell teach or suggest these elements of claim 42. Rather, Leon teaches a system with a single SMD at each user PC. As a result, there is a one to one ratio between users and SMDs. Gravell teaches a system with a single data center with a single key management server." Appeal Br. 13. We disagree with Appellants. We find that a person with ordinary skill in the art would know that since Leon discloses plural SMDs, albeit each associated with a single PC, it nevertheless provides a teaching for using a plurality of Data Centers 30 taught by Gravell to process value bearing item transactions from plural users.

Appellants argue claims 51, 52, 78, 79, 113 and 114 and claims 43-50, 53-56, 59, 60, 64-68, 70, 73-77, 80-83, 86, 87, 91-93, 95-98, 100-102, 105-112 and 115-119 based on Appellants' arguments advanced above for claims 42, 72 and 104. Since we did not find those arguments persuasive, we likewise sustain the rejection of these claims for the same reasons.

CONCLUSIONS OF LAW

We conclude the Appellants have shown that the Examiner erred in rejecting claim 34 under 35 U.S.C. 103(a) as being unpatentable over Leon in view of Gravell.

We conclude the Appellants have not shown that the Examiner erred in rejecting claims 1-33, 35-120 under 35 U.S.C. 103(a) as being unpatentable over Leon in view of Gravell.

DECISION

To summarize, our decision is as follows:

The decision of the Examiner to reject claims 1-33, 35-120 is AFFIRMED.

The decision of the Examiner to reject claim 34 is REVERSED.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv) (2007).

AFFIRM IN PART.

mev

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA CA 91109-7068